KI-RICHTLINIE

für dein Unternehmen

8-Punkte-Vorlage zur EU-AI-Act-Konformität

Eine Arbeitsvorlage aus dem Lehrgang

Manager:in für angewandte KI-Transformation (IHK)

thekey.academy

Stand: 12. Mai 2026 • Version 1.0

Einführung

Diese Vorlage strukturiert eine vollständige KI-Richtlinie für Ihr Unternehmen entlang der acht Pflichtbereiche, die der EU AI Act (Verordnung (EU) 2024/1689) und ergänzende Compliance-Standards adressieren.

Die Vorlage ersetzt keine individuelle juristische Beratung. Sie ist als Arbeitshilfe konzipiert, mit der Sie binnen weniger Stunden eine erste belastbare Fassung Ihrer KI-Richtlinie erstellen können. Anschließend ist eine fachliche Prüfung durch Ihre Rechtsabteilung oder eine externe Kanzlei dringend zu empfehlen.

Aufbau

- Acht thematische Sektionen, die zusammen eine vollständige KI-Richtlinie ergeben.
- Platzhalter in eckigen Klammern [BEZEICHNER] markieren Stellen, an denen unternehmensspezifische Angaben einzusetzen sind.
- Verweise auf konkrete Artikel der KI-Verordnung sind in den jeweiligen Sektionen ausgewiesen.
- Anhang A enthält die wichtigsten Fristen 2025–2027, Anhang B die Lehrgangs-Referenz.

Verwendung

Bearbeiten Sie die Sektionen in der vorgeschlagenen Reihenfolge. Sektion 1 (Geltungsbereich) und Sektion 2 (Governance) bilden die organisatorische Grundlage; Sektion 3 (Risikoklassifizierung) ist Voraussetzung für alle weiteren Pflichten. Sektionen 4–8 können in beliebiger Reihenfolge ergänzt werden.

Wir empfehlen, eine erste Fassung gemeinsam mit Geschäftsführung, IT-Leitung und Datenschutzbeauftragten zu erarbeiten und sie anschließend in einer Stakeholder-Runde mit Personalwesen, Compliance und Betriebsrat zu schärfen.

1. Geltungsbereich und Zweck

1.1 Geltungsbereich

Diese KI-Richtlinie gilt für sämtliche Mitarbeitenden, Auftragnehmenden und Praktikant:innen von [UNTERNEHMENSNAME] sowie für alle KI-Systeme, die durch Mitarbeitende dienstlich genutzt, in Geschäftsprozesse integriert oder auf der Infrastruktur des Unternehmens betrieben werden.

Die Richtlinie umfasst sowohl im Unternehmen entwickelte KI-Systeme („Eigenentwicklung") als auch eingekaufte oder als SaaS bezogene KI-Tools („Drittanbieter-Tools").

> *[Falls Tochtergesellschaften, Joint Ventures oder externe Dienstleister einbezogen werden sollen, listen Sie diese hier auf]*

1.2 Zweck

Die Richtlinie verfolgt vier Ziele:

- Sicherstellung der Konformität mit der EU-KI-Verordnung (Verordnung (EU) 2024/1689) und ergänzenden Vorschriften (DSGVO, BDSG, branchenspezifische Regelungen).
- Schutz vor Reputations-, Haftungs- und Sicherheitsrisiken durch den Einsatz von KI-Systemen.
- Klare Verantwortlichkeiten und Eskalationswege für Mitarbeitende, die KI-Systeme einsetzen oder über deren Einsatz entscheiden.
- Förderung eines verantwortungsvollen, transparenten und nutzbringenden Einsatzes von KI im Unternehmen.

1.3 Ausnahmen

Nicht in den Geltungsbereich fallen ausschließlich für private Zwecke genutzte KI-Tools auf privaten Geräten ohne Verarbeitung von Unternehmensdaten.

> *[Listen Sie hier weitere Ausnahmen auf, z. B. Forschungs-Pilotprojekte mit gesondertem Genehmigungsverfahren]*

1.4 Inkrafttreten

Diese Richtlinie tritt am [DATUM] in Kraft. Sie wird mindestens einmal jährlich überprüft und bei wesentlichen Änderungen der Rechtslage oder der Geschäftstätigkeit angepasst.

2. Verantwortlichkeiten und Governance

2.1 Rollen und Verantwortlichkeiten

Die Verantwortung für die Umsetzung dieser Richtlinie verteilt sich auf folgende Rollen:

Rolle	Verantwortung
Geschäftsführung	Gesamtverantwortung, strategische Freigaben, Sicherstellung der Ressourcenausstattung
KI-Beauftragte:r	Operative Steuerung, Risikobewertung, Schulungsplanung, Berichtspflicht an die Geschäftsführung
IT-Leitung	Technische Implementierung, Sicherheits- und Logging-Maßnahmen, Tool-Bereitstellung
Datenschutzbeauftragte:r	DSGVO-Schnittstellen, Datenverarbeitungsverzeichnis, Datenschutz-Folgenabschätzungen
Fachbereichsleitung	Identifikation von KI-Use-Cases im eigenen Bereich, Vor-Freigabe, Schulungsteilnahme der Mitarbeitenden
Mitarbeitende	Einhaltung der Richtlinie, Meldepflicht bei Vorfällen, Teilnahme an Pflichtschulungen

2.2 KI-Beauftragte:r

Das Unternehmen benennt eine:n KI-Beauftragte:n als zentralen Ansprechpartner für alle Fragen rund um den Einsatz von KI-Systemen. Die Funktion kann mit anderen Rollen kombiniert werden (z. B. Datenschutzbeauftragte:r, IT-Leitung), sofern keine Interessenskonflikte bestehen.

> *[Name und Kontakt der:s KI-Beauftragten eintragen]*

2.3 Risikobewertungs-Pflicht (Art. 9 EU AI Act)

Vor Einführung eines KI-Systems mit potenziellem Risiko erfolgt eine dokumentierte Risikobewertung durch die:den KI-Beauftragte:n in Abstimmung mit den betroffenen Fachbereichen. Die Bewertung berücksichtigt insbesondere:

- Risikoklassifizierung gemäß Sektion 3
- Datenverarbeitung und betroffene Personenkategorien
- Auswirkungen auf Mitarbeitende, Kunden und Dritte
- Notwendige Maßnahmen zur Risikominderung

Die Risikobewertung wird mindestens jährlich oder bei wesentlichen Änderungen aktualisiert.

3. KI-Risiko-Klassifizierung

Der EU AI Act unterscheidet vier Risikoklassen. Jedes im Unternehmen eingesetzte KI-System ist einer dieser Klassen zuzuordnen. Die Klassifizierung erfolgt durch die:den KI-Beauftragte:n vor Inbetriebnahme.

3.1 Die vier Risikoklassen

Klasse	Beispiele	Rechtsfolge
Verbotene Praktiken (Art. 5)	Social Scoring, manipulative Verhaltensbeeinflussung, biometrische Echtzeit-Überwachung im öffentlichen Raum (mit Ausnahmen)	Vollständig untersagt
Hochrisiko-Systeme (Art. 6, Anhang III)	KI in Personalauswahl, Kreditwürdigkeitsprüfung, kritischer Infrastruktur, Strafverfolgung, Bildungsbewertung	Konformitätsbewertung, Registrierung, kontinuierliche Überwachung, Dokumentationspflicht
Begrenztes Risiko	Chatbots im Kundenservice, KI-generierte Inhalte für Marketing	Transparenz- und Kennzeichnungspflicht (siehe Sektion 7)
Minimales Risiko	Rechtschreibprüfung, Spam-Filter, KI-gestützte Spielsoftware	Keine spezifischen Pflichten; freiwillige Selbstverpflichtung empfohlen

3.2 Klassifizierungs-Prozess

1. Fachbereich meldet geplanten KI-Einsatz an die:den KI-Beauftragte:n.
2. KI-Beauftragte:r prüft anhand des Klassifizierungs-Schemas und der Anhänge der EU-KI-Verordnung.
3. Bei Hochrisiko-Einstufung: Einbindung von Datenschutz und Rechtsabteilung; Konformitätsbewertung gemäß Art. 16 ff.
4. Dokumentation der Klassifizierungsentscheidung im KI-Register (siehe Sektion 8).

[Verlinken Sie hier auf Ihr internes KI-Register oder das Datenverarbeitungsverzeichnis]

4. Genehmigte KI-Tools und Vendor-Auswahl

4.1 Tool-Whitelist

Nur ausdrücklich freigegebene KI-Tools dürfen für dienstliche Zwecke genutzt werden. Eine aktuelle Liste der freigegebenen Tools ist über [INTERNER LINK] abrufbar.

> *[Beispielhafte Whitelist: Microsoft 365 Copilot (Enterprise), Anthropic Claude (Team), Google Workspace mit Gemini, ...]*

4.2 Anforderungs-Kriterien für neue Tools

Vor der Aufnahme eines neuen KI-Tools in die Whitelist sind folgende Kriterien zu prüfen:

- Anbieter mit dokumentierter Sicherheits- und Datenschutz-Compliance (ISO 27001, SOC 2, EU-Datenresidenz wo erforderlich)

- Vertraglich zugesicherter Schutz vor Verwendung von Eingabedaten zu Trainingszwecken
- Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 DSGVO
- Risikoeinstufung gemäß Sektion 3
- Belastbare Aussage zur Modell-Erklärbarkeit und zu Maßnahmen gegen Halluzinationen
- Anbieter-Standort und anwendbares Recht (insbesondere bei Drittlandstransfers)

4.3 Verbot von Schatten-KI

Die Nutzung nicht freigegebener KI-Tools – insbesondere kostenfreier Consumer-Versionen wie ChatGPT Free, Gemini Free oder vergleichbare Dienste – ist für dienstliche Zwecke untersagt. Dies gilt insbesondere für die Verarbeitung personenbezogener Daten oder vertraulicher Unternehmensinformationen.

Verstöße werden mit den arbeitsrechtlich zulässigen Mitteln geahndet. Die Geschäftsführung wird auf Verlangen einzelner Bereiche prüfen, ob ein bislang nicht freigegebenes Tool aufgenommen werden kann.

4.4 Genehmigungsverfahren für neue Tools

[Beschreiben Sie den Workflow: Antragsweg, Bearbeitungsfrist, Eskalation]

5. Datenschutz und Daten-Governance

5.1 DSGVO-Schnittmenge

Der EU AI Act ersetzt nicht die DSGVO; beide Regelwerke gelten parallel. Bei jeder KI-Anwendung mit Personenbezug sind beide Compliance-Pfade einzuhalten. Insbesondere:

- Rechtsgrundlage für die Verarbeitung (Art. 6 DSGVO) ist zu dokumentieren.
- Bei Hochrisiko-KI mit personenbezogenen Daten ist eine Datenschutz-Folgenabschätzung (Art. 35 DSGVO) durchzuführen.
- Betroffenenrechte (Auskunft, Löschung, Widerspruch) bleiben vollumfänglich gewahrt.

5.2 Was darf in KI-Systeme eingegeben werden

Grundsätzlich sind folgende Kategorien vor der Eingabe in ein KI-System zu prüfen:

Datenkategorie	Eingabe erlaubt?	Auflagen
Öffentlich verfügbare Daten	Ja	Quellenangabe bei späterer Verwendung
Allgemeine Geschäftsdaten	Ja, in freigegebenen Tools	Nur Whitelist-Tools (Sektion 4.1)
Personenbezogene Daten von Mitarbeitenden/Kunden	Eingeschränkt	Nur mit DSFA und Rechtsgrundlage; nicht in Consumer-Tools
Besondere Kategorien (Art. 9 DSGVO: Gesundheit, Religion, …)	Nur in begründeten Ausnahmen	Vorab schriftliche Freigabe durch DSB
Geschäftsgeheimnisse / vertrauliche Strategie-Dokumente	Nur in vertraglich gesicherten Tools mit No-Training-Klausel	Vorab Freigabe KI-Beauftragte:r
Quellcode / Proprietäre Algorithmen	Eingeschränkt	Vorab Freigabe IT-Leitung und ggf.

Datenkategorie	Eingabe erlaubt?	Auflagen
		Rechtsabteilung

5.3 Datenqualität (Art. 10 EU AI Act)

Für Hochrisiko-KI-Systeme gilt eine erweiterte Datenqualitäts-Pflicht. Die für Training, Validierung und Tests verwendeten Datensätze müssen:

- Relevant, repräsentativ und – soweit möglich – fehlerfrei sein
- Statistische Eigenschaften besitzen, die für den vorgesehenen Verwendungszweck angemessen sind
- Geografische, kontextuelle und funktionale Besonderheiten berücksichtigen
- Möglichst frei von Verzerrungen (Bias) sein, die zu Diskriminierung führen können

Die Erfüllung dieser Anforderungen ist im KI-Register (Sektion 8.3) zu dokumentieren.

6. Mitarbeiter-Kompetenz (KI-Kompetenz-Pflicht, Art. 4)

6.1 Rechtsgrundlage

Seit dem 2. Februar 2025 verpflichtet Art. 4 EU AI Act Anbieter und Betreiber von KI-Systemen, ein ausreichendes Maß an KI-Kompetenz bei ihren Mitarbeitenden sicherzustellen. Die Pflicht trifft das gesamte Unternehmen, unabhängig von Branche oder Größe.

6.2 Zielgruppe und Inhalt

Alle Mitarbeitenden, die KI-Systeme nutzen oder über deren Einsatz entscheiden, durchlaufen eine grundlegende KI-Kompetenz-Schulung. Inhalte sind:

- Grundverständnis der eingesetzten KI-Technologien und ihrer Funktionsweise
- Risikokategorien des EU AI Act und ihre praktische Bedeutung
- Menschliche Aufsicht und Eingriffsmöglichkeiten
- Datenschutz- und Transparenz-Pflichten im Kontext KI
- Konkrete Verhaltensregeln dieser Richtlinie
- Meldewege bei Vorfällen oder Verdachtsfällen

6.3 Schulungs-Häufigkeit und Nachweis

Die Erstschulung erfolgt bei Einstellung bzw. bei Inkrafttreten dieser Richtlinie. Eine Auffrischungsschulung findet jährlich oder bei wesentlichen Änderungen statt.

Die Teilnahme wird dokumentiert und ist auf Verlangen der Aufsichtsbehörden nachzuweisen. Die Dokumentation enthält Datum, Inhalt, Teilnehmende und schulendes Format (Präsenz, E-Learning, Webinar).

[Verweis auf das interne Schulungs-System oder den Schulungs-Anbieter (z. B. thekey.academy)]

6.4 Vertiefende Schulungen für Schlüsselrollen

Mitarbeitende in besonders KI-relevanten Funktionen (IT, Recht, Compliance, Personalwesen, Geschäftsleitung, Fachbereichsleitung) absolvieren vertiefende Schulungen. Empfohlene Formate:

- IHK-zertifizierter Lehrgang „Manager:in für angewandte KI-Transformation" (thekey.academy)
- Branchen-spezifische Workshops zu Hochrisiko-Anwendungsfeldern

- Jährliche EU-AI-Act-Updates mit Rechtsabteilung

7. Transparenz und Kennzeichnung

7.1 Grundsatz

Wenn ein:e Mitarbeiter:in KI für die Erstellung von Inhalten, Entscheidungsvorschlägen oder Außenkommunikation einsetzt, ist dies in geeigneter Weise transparent zu machen.

7.2 Konkrete Kennzeichnungspflichten

Anwendungsfall	Pflicht zur Kennzeichnung	Rechtsgrundlage
Chatbot im Kundenservice	Ja: „Sie sprechen mit einem KI-Assistenten" oder Ähnliches	Art. 50 (1) EU AI Act
KI-generierte Bilder/Videos in externer Kommunikation	Ja, wenn Personen abgebildet werden oder Inhalte als real erscheinen könnten (Deepfake-Regel)	Art. 50 (4) EU AI Act
KI-generierte Texte in Marketing	Empfohlen, jedoch nicht überall verpflichtend	Branchen-Selbstverpflichtungen
KI-gestützte Entscheidungen mit Außenwirkung (z. B. Kreditprüfung)	Ja, Betroffene sind zu informieren	Art. 13–14 EU AI Act + Art. 22 DSGVO
Interne Entscheidungsvorschläge (z. B. Bewerbung-Vorsortierung)	Ja, gegenüber Endentscheider:in	Art. 14 EU AI Act

7.3 Deepfake-Regelung (Art. 50)

Bild-, Audio- oder Video-Inhalte, die durch KI erzeugt oder manipuliert wurden und Personen oder Ereignisse fälschlich darstellen könnten („Deepfakes"), sind in jedem Fall als solche zu kennzeichnen. Ausnahmen gelten ausschließlich für künstlerische, satirische oder fiktionale Inhalte mit eindeutiger Kontextualisierung.

7.4 Interne Kennzeichnung

Auch unternehmensintern soll der Einsatz von KI-Tools bei der Erstellung von Dokumenten transparent gemacht werden – etwa durch eine Anmerkung am Ende eines Dokumentes („Dieser Entwurf wurde KI-gestützt erstellt und durch [Name] redaktionell überarbeitet").

8. Incident-Reporting und Audit

8.1 Meldepflicht bei Vorfällen

Jede:r Mitarbeiter:in ist verpflichtet, KI-bezogene Vorfälle unverzüglich zu melden. Als Vorfall gelten insbesondere:

- Fehlerhafte oder schädigende Ausgaben eines KI-Systems (z. B. diskriminierende Ergebnisse, falsche Auskünfte mit Außenwirkung)
- Verdacht auf unbefugte Datenabflüsse durch KI-Tools
- Sicherheitsvorfälle: KI-basierte Phishing-Versuche, Deepfake-Angriffe gegen Mitarbeitende
- Verletzungen dieser Richtlinie, die einem oder einer selbst auffallen

8.2 Meldewege

Vorfälle werden gemeldet an:

- Bei akuter Datenschutz-Verletzung: Datenschutzbeauftragte:r (binnen 24 Stunden gemäß Art. 33 DSGVO)
- Bei akutem Sicherheitsvorfall: IT-Leitung (Notfall-Hotline: [TELEFONNUMMER])
- Allgemeine Meldungen: KI-Beauftragte:r ([E-MAIL])
- Anonyme Meldungen: über das Hinweisgeber-System [LINK]

8.3 KI-Register und Audit-Trail

Das Unternehmen führt ein zentrales KI-Register, das mindestens enthält:

- Bezeichnung und Anbieter jedes eingesetzten KI-Systems
- Risikoklassifizierung gemäß Sektion 3
- Verantwortlicher Fachbereich und KI-Beauftragte:r
- Datum der Freigabe und letzten Risikobewertung
- Datenkategorien, die verarbeitet werden
- Kennzeichnungspflichten und -umsetzung
- Dokumentierte Vorfälle und Maßnahmen

8.4 Externe Meldepflichten

Schwerwiegende Vorfälle bei Hochrisiko-KI-Systemen (z. B. Tod, schwere Gesundheitsschäden, Grundrechtsverletzungen, kritische Infrastruktur-Ausfälle) sind gemäß Art. 73 EU AI Act unverzüglich an die zuständige Marktüberwachungsbehörde zu melden. Die Meldung erfolgt durch die:den KI-Beauftragte:n in Abstimmung mit der Geschäftsführung.

8.5 Interne Audits

Mindestens einmal jährlich erfolgt ein internes Audit der KI-Compliance. Der Audit-Bericht wird der Geschäftsführung vorgelegt und führt zu konkreten Maßnahmen für das Folgejahr.

Anhang A: Fristen 2025–2027

Der EU AI Act tritt gestaffelt in Kraft. Die folgende Übersicht fasst die für Unternehmen wichtigsten Stichtage zusammen.

Datum	Was tritt in Kraft	Was Unternehmen jetzt tun
02.02.2025	Verbot bestimmter KI-Praktiken (Art. 5); KI-Kompetenz-Pflicht (Art. 4)	Schulungs-Konzept aufsetzen, Whitelist prüfen
02.08.2025	Pflichten für General-Purpose-AI-Modelle (GPAI)	Vertragspartner-Verträge auf GPAI-Klauseln prüfen
02.02.2026	Verhaltenskodizes treten in Kraft	Brancheninitiativen beobachten
02.08.2026	Pflichten für Hochrisiko-KI-Systeme nach Anhang III	Konformitätsbewertungen durchführen, Registrierung
02.08.2027	Volle Anwendung auf vor 02.08.2026 bereits im Verkehr befindliche Systeme	Bestandsaufnahme aller älteren Systeme abschließen

Quelle: Verordnung (EU) 2024/1689 (EU AI Act), Art. 113. Aktualisierungen sind auf der Website der Europäischen Kommission und auf den Seiten der Bundesnetzagentur (als zuständige deutsche Marktüberwachungsbehörde nach KI-Diensteanbieter-Gesetz) zu verfolgen.

Anhang B: Lehrgangsbezug und Disclaimer

Herkunft dieser Vorlage

Diese Richtlinien-Vorlage ist eine Arbeitshilfe aus dem Lehrgang Manager:in für angewandte KI-Transformation (IHK) bei thekey.academy. Die Inhalte werden in Modul 8 „Exkurs: Fit für die KI-VO" – insbesondere in der Lektion „Erstellung einer KI-Richtlinie für das Unternehmen" – im Detail vermittelt und an praktischen Fallbeispielen geübt.

Lehrgangs-Eckdaten:

- 9 Module, 91 Lektionen, ca. 15,9 Stunden Lerninhalt
- Selbstlerntempo, 100 % online
- IHK-Zertifikat als Abschluss
- Dediziertes EU-AI-Act-Modul mit acht Lektionen
- Dozent:innen: Andrea Grießmann, Christopher Kuhl, Dr. Harald Feldkamp, Eva Wolfangel

Rechtlicher Hinweis

Diese Vorlage ist eine Arbeitshilfe. Sie ersetzt keine individuelle juristische Beratung. Die konkrete Anpassung an die Unternehmenssituation, das Geschäftsmodell, die eingesetzten KI-Systeme und die anwendbaren branchenspezifischen Vorschriften ist erforderlich.

thekey.academy übernimmt keine Haftung für die Verwendung dieser Vorlage. Wir empfehlen vor der Verabschiedung der unternehmensspezifischen Richtlinie eine Prüfung durch eine im IT-Recht erfahrene Rechtsabteilung oder Kanzlei.

Aktualisierung

Dokumenten-Version 1.0 · Stand: 12. Mai 2026 · Nächste planmäßige Aktualisierung: November 2026.

Bei wesentlichen Änderungen der Rechtslage – insbesondere durch Konkretisierungs-Verordnungen der Europäischen Kommission, nationale Umsetzungsgesetze oder höchstrichterliche Rechtsprechung – erfolgt eine außerplanmäßige Aktualisierung.